IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

ContentGuard Holdings, Inc., *Plaintiff*, v. Amazon.com, Inc.; Apple Inc.; BlackBerry Limited (fka Research In Motion Limited) and BlackBerry Corporation (fka Research In Motion Corporation); HTC Corporation and HTC America, Inc.; Huawei Technologies Co., Ltd. and Huawei Device USA, Inc.; Motorola Mobility LLC; Samsung Electronics Co., Ltd., Samsung Electronics America, Inc., and Samsung Telecommunications America, LLC, *Defendants*.	Civil Action No. 2:13-cv-01112-JRG JURY TRIAL DEMANDED

JOINT MOTION FOR ENTRY OF A PROTECTIVE ORDER

Plaintiff, ContentGuard Holdings, Inc. ("ContentGuard") and Defendants Amazon.com, Inc., Apple Inc., BlackBerry Limited, BlackBerry Corporation, HTC Corporation, HTC America, Inc., Huawei Technologies Co., Ltd., Huawei Device USA, Inc., Motorola Mobility LLC, Samsung Electronics Co., Ltd., Samsung Electronics America, Inc., and Samsung Telecommunications America, LLC (collectively "Defendants") were able to agree on many provisions of the Protective Order except for the following Disputed Provisions:

1. Paragraph 1(b) – Purposes and Limitations
2. Paragraph 6(b) – Patent Prosecution Bar
3. Paragraph 6(c) – Secure Storage, No Export
4. Paragraph 6(f) – Cross-Production of Defendant Confidential Material

5. Paragraph 8(c)(iii) – Discovery Material Designated as "Confidential"

6. Paragraph 9(d)(i) – Discovery Material Designated as "Confidential – Outside Attorneys' Eyes Only"

7. Paragraph 9(d)(ii) – Discovery Material Designated as "Confidential – Outside Attorneys' Eyes Only"

8. Paragraph 10(c)(i) - Discovery Material Designated as "Confidential – Outside Attorneys' Eyes Only – Source Code"

9. Paragraph 10(c)(ii) - Discovery Material Designated as "Confidential – Outside Attorneys' Eyes Only – Source Code"

10. Paragraph 11(b) - Disclosure and Review of Source Code

11. Paragraph 11(c)(i) - Disclosure and Review of Source Code

12. Paragraph 11(c) - Disclosure and Review of Source Code

13. Paragraph 11(c)(ii) - Disclosure and Review of Source Code

14. Paragraph 11(c)(iv) - Disclosure and Review of Source Code

15. Paragraph 11(c)(viii) - Disclosure and Review of Source Code

16. Paragraph 11(x) - Disclosure and Review of Source Code

17. Paragraph 11(xi) - Disclosure and Review of Source Code

18. Paragraph 12(a) – Third-Party Confidentiality Obligations

19. Paragraph 13(a)(iv) – Notice of Disclosure

20. Paragraph 13(a) – Notice of Disclosure

ContentGuard's proposed Protective Order is attached as Exhibit A. Defendants' proposed Protective Order is attached as Exhibit B. Where differences exist, Plaintiff and Defendants have listed their competing proposals in the tables below with the disputed language underlined. Additionally, Plaintiff's and Defendants' respective positions on the disputed provisions are set forth below. As set forth below, the parties are not presenting twenty separate disputes for the Court to resolve. Rather, as their titles suggest, the disputed provisions contain overlapping language and issues.

Accordingly, the parties respectfully request that the Court enter a Protective Order and resolve the disputed language where indicated.

1. Paragraph 1(b) – Purposes and Limitations

Plaintiff's Proposal	Defendants' Proposal
To the extent that any one of Defendants in this litigation provides Protected Material under the terms of this Protective Order to Plaintiff, Plaintiff shall not share that material with the other Defendants in this litigation, absent express written permission from the producing Defendant. Notwithstanding the foregoing, Plaintiff and Defendants may disclose one Defendant's Protected Material and Protected Material disclosed by Google Inc. in the co-pending *ContentGuard v Google* case to any other Defendants' Outside Counsel, Outside Counsel for Google, Inc., and retained experts through Court filings, oral argument in Court, expert reports, depositions, discovery requests, discovery responses, or any other means, so long as the disclosure is designated "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY" in accordance with this Order. This Order does not confer any right to any one Defendant to access the Protected Material of any other Defendant.	To the extent that any one of Defendants in this litigation provides Protected Material under the terms of this Protective Order to Plaintiff, Plaintiff shall not share that material with the other Defendants in this litigation, absent express written permission from the producing Defendant, which permission shall not be unreasonably withheld. This Order does not confer any right to any one Defendant to access the Protected Material of any other Defendant.

Plaintiff's Statement:

ContentGuard anticipates that it will need to use Protected Material produced by certain Defendants against other Defendants. By way of example, because the Amazon Kindle app is preinstalled on certain Samsung devices, ContentGuard may need to use Amazon-produced documents concerning the Kindle app to prove Samsung's infringement. Along the same lines, ContentGuard may need to use Google-produced documents to prove infringement by Defendants such as Samsung or Motorola, who incorporate Google-made software in their devices. To address the need for such cross-disclosure while at the same time ensuring that Defendants' Protected Material remains safeguarded, ContentGuard proposes allowing the

parties to disclose Protected Material produced by any Defendant or Google to any other Defendants' Outside Counsel, Google's Outside Counsel, and retained experts but not to any other Defendant in this action or Google, i.e. their in-house counsel, or corporate representatives. ContentGuard respectfully submits that, in combination with other provisions of the Protective Order, this approach ensures that Defendants' Protected Material remains in strict confidence and is not misused.

In contrast, Defendants' proposed language is unworkable as a practical matter because it prevents ContentGuard from filing motions, propounding discovery, or submitting expert reports across the Defendants in this litigation without going through the cumbersome process of obtaining prior written approval. The effect of Defendants' proposed language is that ContentGuard is unduly saddled with the obligation to vet and pre-clear with Defendants filings that may raise cross-disclosure issues and in some cases submit redacted or separate filings/reports/discovery depending on the Defendant that may access them. Because each Defendant will inevitably seek access to all of ContentGuard's filings, expert reports, and discovery, ContentGuard's proposal allows that access without incurring any additional cost or time seeking permission and potentially disputing whether that permission was unreasonably withheld.

Defendants' Statement:

Plaintiff proposes in this and other provisions that it should be permitted to share one Defendant's Protected Material with the counsel and experts retained by other Defendants. Defendants object to providing Plaintiff with such discretion absent notice because all of the Defendants are direct competitors who could suffer severe competitive harm from such disclosures of Protected and trade secret information. Put simply, Amazon, Apple, and Google

do not consent to Plaintiff sharing their respective trade secret, DRM Protected Materials between representatives of these direct competitors. Likewise, Amazon, Apple, Blackberry, HTC, Huawei, Motorola and Samsung also do not consent to Plaintiff sharing their trade secret, hardware Protected Materials between representatives of these direct competitors. In the event Plaintiff desires to disclose the Protected Material of a Defendant to the representatives of another Defendant, the protective order should require that Plaintiff seek the producing Defendant's consent. Additionally, Plaintiff should not be permitted to circumvent this Court's denial of the motion to consolidate the Google matter with this matter by sharing Protected Materials between the cases without notice and an opportunity to object. *See* Dkt. No. 109 at 9.

Permitting Plaintiff unfettered ability to share any one Defendant's Protected Material with any other Defendant's hired expert effectively forces all Defendants to only select experts that are acceptable to every single other Defendant. For instance, BlackBerry may wish to hire an expert who is objectionable to Apple on the basis of that expert's other current or recent work. If Plaintiff's proposed language on this provision is adopted, Apple may be forced to object to BlackBerry's desired expert. Plaintiff would therefore hamper each Defendants' ability to effectively defend itself.

2. Paragraph 6(b) – Patent Prosecution Bar

Plaintiff's Proposal	Defendants' Proposal
Absent the written consent of the Producing Party, any attorney representing a Party, whether in-house or outside counsel, and any person associated with a Party and permitted to receive the other Party's Protected Material that is designated "CONFIDENTIAL - OUTSIDE ATTORNEYS' EYES ONLY" or "CONFIDENTIAL - OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" (collectively "HIGHLY SENSITIVE MATERIAL"), who obtains, receives, has access to, or otherwise learns, in whole or in part, the other Party's HIGHLY SENSITIVE MATERIAL under this Order shall not prepare, prosecute, supervise, or assist in the preparation or prosecution of any patent application relating to the functionality, operation, and design of digital rights management ("DRM") systems and methods as used in Defendants' products on behalf of the receiving Party or its acquirer, successor, predecessor, or other affiliate during the pendency of this Action and for one year after its conclusion, including any appeals. To ensure compliance with the purpose of this provision, each Party shall create an "Ethical Wall" between those persons with access to HIGHLY SENSITIVE MATERIAL and any individuals who, on behalf of the Party or its acquirer, successor, predecessor, or other affiliate, prepare, prosecute, supervise or assist in the preparation or prosecution of any patent application relating to the functionality, operation, and design of digital rights management systems and methods as used in Defendants' products.	Absent the written consent of the Producing Party, any attorney representing a Party, whether in-house or outside counsel, and any person associated with a Party and permitted to receive the other Party's Protected Material that is designated "CONFIDENTIAL - OUTSIDE ATTORNEYS' EYES ONLY" or "CONFIDENTIAL - OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" (collectively "HIGHLY SENSITIVE MATERIAL"), who obtains, receives, has access to, or otherwise learns, in whole or in part, the other Party's HIGHLY SENSITIVE MATERIAL under this Order shall not prepare, prosecute, supervise, or assist in the preparation or prosecution of any patent application relating to the functionality, operation, and design of digital rights management ("DRM") and digital content distribution systems and methods, including associated software and hardware (generally or as described in any patent in suit) during the pendency of this Action and for two years after its conclusion, including any appeals. To ensure compliance with the purpose of this provision, each Party shall create an "Ethical Wall" between those persons with access to HIGHLY SENSITIVE MATERIAL and any individuals who, on behalf of the Party or its acquirer, successor, predecessor, or other affiliate, prepare, prosecute, supervise or assist in the preparation or prosecution of any patent application relating to the functionality, operation, and design of digital rights management systems and methods as used in Defendants' products.

Plaintiff's Statement:

The parties' dispute concerns the scope of the prosecution bar and its duration. ContentGuard's proposal faithfully tracks this Court's Model Protective Order by: (1) defining the scope of the bar broadly enough to cover the subject matter of this litigation, but narrowly enough not to apply to unrelated subject matter; (2) limiting the bar to patent prosecution activities conducted "on behalf of the receiving Party or its acquirer, successor, predecessor, or other affiliate," as opposed to unrelated third-parties; and (3) fixing the duration of the bar to one year. In contrast, Defendants' competing proposal materially deviates from the Model Protective Order and extends the scope of prohibited activities well beyond what is reasonable and appropriate. We address each aspect of the parties' disputes in turn.

First, Defendants wish for the bar to apply not only to "DRM systems and methods" but also to any "digital content distribution systems and methods, including associated software and hardware." Applied literally, however, this extraordinarily sweeping bar would prohibit the recipients of confidential information (attorneys, consultants, and experts) from participating in patent prosecution activities covering any hardware device or software used in the distribution of digital content, which in effect means all hardware and software made, used and sold today, even if the prosecution activities in question in such hardware or software cover subject matter that has nothing to do with DRM as used in Defendants' products. Thus, by way of example, recipients of confidential information would be prohibited from prosecuting patents concerning screens, keyboards, batteries, and myriad other aspects or elements of "hardware" that are unrelated to the subject matter of this litigation, *i.e.*, DRM. ContentGuard respectfully submits that such a broad prohibition is unwarranted because it would foreclose ContentGuard's

attorneys, consultants, and experts from engaging in patent prosecution activities that are wholly unrelated to the subject matter of this litigation.

Second, Defendants wish to apply the bar not only to prosecution activities conducted "on behalf of the receiving Party or its acquirer, successor, predecessor, or other affiliate," as specified in this Court's Model Protective Order, but also to activities conducted on behalf of unrelated third-parties. But because the Protective Order makes clear that all confidential information produced in this case "shall be used by a Receiving Party solely for this case, and shall not be used directly or indirectly for any other purpose whatsoever," there is no legitimate reason to extend the prosecution bar as Defendants propose.

Third, Defendants wish for the bar to last two years. ContentGuard respectfully submits that the one year timeframe specified in the Court's Model Protective Order is more appropriate. This is particularly true given that the Protective Order makes clear that confidential information produced in this case "shall be used by a Receiving Party solely for this case, and shall not be used directly or indirectly for any other purpose whatsoever." In other words, even after the expiration of the prosecution bar period, Defendants' confidential information will remain off-limits for all purposes.

Defendants' Statement:

All parties agree, consistent with Federal Circuit precedent, that a patent prosecution bar is necessary in this case. *See In re Deutsche Bank Trust*, 605 F.3d 1373, 1377-78 (Fed. Cir. 2010). The dispute concerns the scope of the Protected Material that Plaintiff intends to seek in this case, and whether the bar should continue for one or two years.

The Defendants' proposed prosecution bar is reasonable and necessary because Plaintiff has identified in its complaint and infringement contentions not only digital rights management

("DRM") software, but also hundreds of hardware smart phones, tablets, and other computing devices that it contends are DRM protected devices. As this Court has recognized, Plaintiff's allegations are less than clear concerning the extent to which hardware, as opposed to software, is relevant. Dkt. No. 109. Nevertheless, Plaintiff's complaint identifies the Apple iPad, Amazon Kindle Fire, the BlackBerry Z10, the HTC One Max, the Huawei Ascend, the Motorola Moto X, and the Samsung Galaxy S4. Dkt. No. 22. Defendants have already produced substantial Protected Materials based on Plaintiff's disclosures. The Defendants' proposed language (("functionality, operation, and design of digital rights management ("DRM") and digital content distribution systems and methods, *including associated software and hardware (generally or as described in any patent in suit)*") prohibits Plaintiff's counsel from participating in prosecution or acquisition of patents that concern technology that Plaintiff has expressly accused, while simultaneously having access to Protected Materials on such technology produced in this case. The proposed bar's subject matter limitation is of limited scope commonly seen in protective orders in this Court. *See, e.g.*, Agreed Prot. Order at ¶ 8, *Affinity Labs of Tex., LLC v. Nike, Inc.*, No. 2:10-cv-54, ¶ 8 (E.D. Tex. Aug. 3, 2010) ("relating to either the technology of the Patents-in-Suit or…").[1] Any burdens on Plaintiff are minimized by limiting the scope to only those matters relevant to the subject matter of this lawsuit as defined by Plaintiff itself. In contrast, Plaintiff's proposal seeks to limit the bar to DRM ("functionality, operation, and design of digital rights management systems and methods as used in Defendants' products") which is far narrower than the technologies that Plaintiff accuses.

Plaintiff's second argument, that counsel can segregate their knowledge from this case in work for other clients, in untenable. The prosecution bar itself recognizes that the risk of

[1] The *Affinity Labs* protective order is available in the attached May 16, 2014 Greenblatt Decl. at Ex. 1.

inadvertent use of Protected Information during patent prosecution requires more than a general prohibition against using such information beyond this case. Avoiding use of Protected Information when it would be helpful in counsel's work is nearly impossible, as the Federal Circuit clearly observed in *In re Deutsche Bank*. *Id*. at 1380-81. In *Deutsche Bank*, the Court recognized that an attorney in possession of an opponent's confidential information should be barred from certain activities before the PTO due to the high risk of even inadvertent misuse of that information. *Id*. Justifying this bar, the Federal Circuit reasoned that "it is very difficult for the human mind to compartmentalize and selectively suppress information once learned, no matter how well-intentioned the effort may be to do so." *Id.* at 1378. Plaintiff's proposal presents exactly the sort of untenable situation the Federal Circuit has found to warrant a prosecution bar: "Courts have recognized [] that there may be circumstances in which even the most rigorous efforts of the recipient of such information to preserve confidentiality … may not prevent inadvertent compromise." *Id.*

Finally, Defendants proposed two year bar is clearly reasonable and the Court has previously issued Protective Orders with similar provisions. *See, e.g.*, *LG Elecs., Inc. v. Petters Group Worldwide, L.L.C.*, 2009 U.S. Dist. LEXIS 38735, at *9-10 (E.D. Tex. May 7, 2009) ("two years after the conclusion of this litigation")[2]; Agreed Prot. Order at ¶ 8, *Affinity Labs of Tex., LLC v. Nike, Inc.*, No. 10-54, at ¶¶ 8, 9(b) (E.D. Tex. August 3, 2010), ECF No. 55 ("two (2) years after the final res[o]lution of this action")[3]; Stip. Prot. Order at ¶ 5(a)(ii), *Allergan, Inc. v. Watson Labs., Inc.*, No. 10-344, at ¶ 5(ii) (E.D. Tex. Jan. 13, 2011), ECF No. 23 ("two (2) years from final disposition of this action")[4]; *Keystone Autonics, Inc. v. Sirius Satellite Radio*

[2] The *LG Elecs.* protective order is available in the Greenblatt Decl. at Ex. 2.

[3] The *Affinity Labs* protective order is available in the Greenblatt Decl. at Ex. 1.

[4] The *Allergan* protective order is available in the Greenblatt Decl. at Ex. 3.

Inc., No. 2:07-cv-61, at ¶ 34 (E.D. Tex. Mar. 4, 2008) ("two (2) years following the final resolution of this lawsuit (either through settlement or judgment including appeals");[5] *Adaptix, Inc. v. Alcatel-Lucent USA, Inc.*, No. 12-022 (E.D. Tex. Aug. 22, 2012) ECF No. 455 ("The Court adopts Defendants' proposal regarding [the] two year duration of the prosecution bar.").

Because Defendants' proposal is tailored to cover the full scope of Protected Materials likely to be produced in this litigation and provides a reasonable period for the prosecution bar, they respectfully request that this Court adopt their proposal.

[5] The *Keystone* protective order is available in the Greenblatt Decl. at Ex. 4.

3. Paragraph 6(c) – Secure Storage, No Export

Plaintiff's Proposal	Defendants' Proposal
Protected Material must be stored and maintained by a Receiving Party at a location in the United States and in a secure manner that ensures that access is limited to the persons authorized under this Order. Each party receiving Protected Information shall comply with all applicable export control statutes and regulations. See, e.g., 15 CFR 734.2(b). Protected Information, exclusive of material designated CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY – SOURCE CODE, and to the extent otherwise permitted by law, may be taken outside the territorial limits of the United States to the extent reasonably necessary for a deposition taken in a foreign country. Notwithstanding the foregoing, the prohibitions of this paragraph shall not apply to persons permitted to receive Protected Information pursuant to paragraph 8(c)(ii) of this Order. The restrictions contained within this paragraph may be amended through the consent of the producing Party to the extent that such agreed to procedures conform with applicable export control laws and regulations.	Protected Material must be stored and maintained by a Receiving Party at a location in the United States and in a secure manner that ensures that access is limited to the persons authorized under this Order. Each party receiving Protected Information shall comply with all applicable export control statutes and regulations. See, e.g., 15 CFR 734.2(b). No Protected Information may leave the territorial boundaries of the United States of America or be made available to any foreign national who is not (i) lawfully admitted for permanent residence in the United States or (ii) identified as a protected individual under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)). No Protected Information may leave the territorial boundaries of the United States of America. Without limitation, this prohibition extends to Protected Information (including copies) in physical and electronic form. The viewing of Protected Information through electronic means outside the territorial limits of the United States of America is similarly prohibited. Notwithstanding this prohibition, Protected Information, exclusive of material designated CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY – SOURCE CODE, and to the extent otherwise permitted by law, may be taken outside the territorial limits of the United States to the extent reasonably necessary for a deposition taken in a foreign country. Notwithstanding the foregoing, the prohibitions of this paragraph shall not apply to persons permitted to receive Protected Information pursuant to paragraph 8(c)(ii) of this Order. The restrictions contained within this paragraph may be amended through the consent of the producing Party to the extent that such agreed to procedures conform with applicable export control laws and regulations.

Plaintiff's Statement:

ContentGuard respectfully opposes the additional language proposed by Defendants for two reasons. First, Defendants' proposal deviates from the Model Protective Order. Second, the Defendants' proposal is unduly restrictive because it would preclude ContentGuard from making use of overseas vendors and lawfully-admitted individuals present in the United States who are not "permanent residents" or refugees. In light of other safeguards set forth in the Protective Order there is no reason for these restrictions, and other courts within this District have rejected very similar provisions. For instance, in *EON Corp. IP Holdings, LLC v. Landis + Gyr Inc.*, 2012 U.S. Dist. 81107 (E.D. Tex. June 12, 2012), the court rejected a provision *less restrictive* than that proposed by Defendants here, which in part read as follows: "Material designated HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY OR HIGHLY CONFIDENTIAL – . . . shall not be disclosed to any person or entity located outside the United States and HIGHLY CONFIDENTIAL MATERIAL shall not be sent, distributed, or otherwise taken to any location outside the United States." *Id.* at *4-5. The Court held that "in light of the safeguards already present in the protective order, Defendants have not shown that their additional proposed safeguards are necessary. . . . As Plaintiff points out, the Protective Order provides strong protection against the dissemination of confidential information." *Id.* at *8-9.

Defendants' Statement:

Defendants' proposal in this section addresses the risk associated with transporting Protected Material to foreign jurisdictions. The Protective Order does not (and cannot) grant any Federal Court personal jurisdiction over persons located in foreign countries necessary to enforce the Protective Order. *See e.g., Westerngeco LLC v. Ion Geophysical Corp.*, 776 F. Supp. 2d 342, 367 n.17 (S.D. Tex. Mar. 2, 2011) ("Although a state may, in limited circumstances, extend its

jurisdiction beyond the territorial limits of its sovereignty, any such extension is 'subject to the consent of other nations.'") (citations omitted).[6]

Should any person outside of the jurisdiction of the Federal Courts misuse confidential information or violate the Protective Order in any manner, the producing party would be powerless to enforce the provisions of the Protective Order against such person. The producing party would be unable to seek relief by, for example, requesting temporary restraining orders or sanctions against the offending persons. Any remedy that could be sought, such as sanctions, would provide effectively no relief at all from competitive harm imposed by foreign nationals. *See e.g., Cruz v. Hauck*, 515 F. 2d 322 (5th Cir. 1975) (in explaining the difference between a judge's error made within her power and a challenge to the court's jurisdiction, the court explained that the latter attacks the court's powers itself and that "[a]n order without power is void"). Simply put, Plaintiff's proposal asks the Court to issue an order that it cannot effectively enforce against foreign consultants who would have access to confidential information.

As set forth in the Declarations of Maxine Curry, Beth Kellerman and Payam Mirrashidi submitted by Apple, Plaintiff's demand that it be free to send confidential information overseas

[6] Federal Courts, including the U.S. Supreme Court, have repeatedly recognized the limits of their power to reach the activities outside of the United States and its territories. *See e.g., Brown v. Duchesne,* 60 U.S. (19 How.) 183, 195 (1856) ("Our patent system makes no claim to extraterritorial effect; these acts of Congress do not, and were not intended to, operate beyond the limits of the United States . . . ." (internal quotation marks omitted)); *Deepsouth Packing Co. v. Laitram Corp*., 406 U.S. 518, 531, 92 S. Ct. 1700, 32 L. Ed. 2d 273 (1972), *superseded by statute*, Patent Law Amendments Acts of 1984, Pub. L. No. 98-622, 98 Stat. 3383 (codified at 35 U.S.C. § 271(f)), *as recognized in Microsoft Corp. v. AT&T Corp*., 550 U.S. 437 (2007); *Power Integrations, Inc., v. Fairchild Semiconductor Int'l Inc.*, 711 F.3d 1348, 1371 (Fed. Cir. 2013) ("It is axiomatic that U.S. patent law does not operate extraterritorially to prohibit infringement abroad.")

presents real competitive and legal risks.[7] Further, the transmission of confidential materials to foreign jurisdictions raises potential concerns with U.S. export control legislation, which prohibits export of certain materials to foreign jurisdictions. Declaration of Maxine Curry, at ¶¶ 5-6.[8] *See e.g., Keystone Autonics, Inc. v. Sirius Satellite Radio Inc.*, No. 2:07-cv-61, at ¶¶ 5, 38 (E.D. Tex. Mar. 4, 2008) (explaining that the parties acknowledged that certain data and information produced and disclosed by the defendants was subject to U.S. laws and regulations, including applicable export laws, and granted the agreed protective order provision that prohibited any produced information to be reviewed by, accessed by or disclosed to any Foreign Person).[9] The protective order should not condone the export of confidential materials describing encryption technology, which is the focus of Plaintiff's claims. Declaration of Maxine Curry, at ¶¶ 5-6; Declaration of Payam Mirrashidi, at ¶ 7.

This Court has previously prohibited parties from sending Confidential Materials to foreign jurisdictions in similar circumstances. In *RMAIL Ltd. v. Amazon.com, Inc.*, No. 2:10- cv-258 (E.D. Tex. June, 18, 2013), the Eastern District of Texas prohibited sending the parties' confidential information to India-based consultants because the parties could use U.S.- based consultants and there was no indication that the U.S.-based consultants had to be limited in number or were otherwise inadequate. *Id.* at *3. Just like in *Amazon*, the "risk of unintentional or intentional dissemination of protected material abroad outweighs any benefit" from use of foreign-based consultants. *Id.* In *EON Corp. IP Holdings, LLC v. LG*

[7] The referenced Declarations are available in the Greenblatt Decl. at Exs. 5, 6 and 7.

[8] *See also* http://www.state.gov/strategictrade/overview/; http://export.gov/regulation/ ; http://www.nyu.edu/research/resources-and-support-offices/getting-started-withyourresearch/office-of-sponsored-programs/policies/export-control-regulations.html; http://doresearch.stanford.edu/research-scholarship/export-controls/research-and-encryption.

[9] The *Keystone* protective order is available in the Greenblatt Decl. at Ex. 4.

Electronics Mobilecomm USA, Inc., 6:12-cv-00941-LED-JDL (E.D. Tex. June 28, 2013), Dkt. Nos. 23-30, 23-31, this Court applied domestic limitations in protective order based on record evidence that iTunes source code contains highly-sensitive encryption technologies, access to which is highly controlled and subject to U.S. export compliance obligations.[10] In contrast, the defendant in *EON Corp. IP Holdings, LLC v. Landis+Gyr Inc.*, No. 6:11-cv-317, at-*4-5 (E.D. Tex. June 12, 2012), failed to establish any risks associated with the protective order permitting the export of their confidential information to foreign consultants.

[10] The referenced Order in *EON Corp. IP Holdings, LLC v. LG Electronics Mobilecomm USA, Inc.*, No. 6:12-cv-00941 (E.D. Tex. July 8, 2013) is available in the Greenblatt Decl. at Ex. 8. *See also* Ex. 2 to the Greenblatt Decl.

4. Paragraph 6(f) – Cross-Production of Defendant Confidential Material

Plaintiff's Proposal	Defendants' Proposal
No Defendant is required to produce its Protected Material to any other Defendant or Defendants, but nothing in this Order shall preclude such production. Notwithstanding the provisions of this Protective Order, Plaintiff shall not disclose one Defendant's Protected Material to any other Defendant or Defendants through Court filings, oral argument in Court, expert reports, deposition, discovery requests, discovery responses, or any other means, without the express prior written consent of the Defendant that produced the Protected Material. Notwithstanding the provisions of this Protective Order, Plaintiff and Defendants may disclose one Defendant's Protected Material to any other Defendants' Outside Counsel or retained experts through Court filings, oral argument in Court, expert reports, deposition, discovery requests, discovery responses, or any other means, so long as the disclosure is designated "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY" in accordance with this Order.	No Defendant is required to produce its Protected Material to any other Defendant or Defendants, but nothing in this Order shall preclude such production. Notwithstanding the provisions of this Protective Order, Plaintiff shall not disclose one Defendant's Protected Material to any other Defendant or Defendants through Court filings, oral argument in Court, expert reports, deposition, discovery requests, discovery responses, or any other means, without the express prior written consent of the Defendant that produced the Protected Material, which permission shall not be unreasonably withheld.

Plaintiff's Statement:

Plaintiff's statement is set forth in Disputed Provision 1 above.

Defendants' Statement:

Defendants' position concerning Plaintiffs' proposal to share Defendants' Protected Materials with other Defendants absent notice is set forth in Section 1(b), above.

5. Paragraph 8(c)(iii) – Discovery Material Designated as "Confidential"

Plaintiff's Proposal	Defendants' Proposal
Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL" may be disclosed only to the following: . . . (iii) Any outside expert or consultant retained by the Receiving Party to assist in this action and supporting personnel, provided that disclosure is only to the extent necessary to perform such work; and provided that: (a) such expert or consultant has agreed to be bound by the provisions of the Protective Order by signing a copy of Exhibit A; (b) no unresolved objections to such disclosure exist after proper notice has been given to all Parties as set forth in Paragraph 13 below. Without the express prior written consent of the Defendant that produced the Protected Material, no expert or consultant retained by a Defendant in this matter shall have access to "CONFIDENTIAL – ATTORNEYS' EYES ONLY" Discovery Material produced by another Defendant in this matter;	Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL" may be disclosed only to the following: . . . (iii) Any outside expert or consultant retained by the Receiving Party to assist in this action, provided that disclosure is only to the extent necessary to perform such work; and provided that: (a) such expert or consultant has agreed to be bound by the provisions of the Protective Order by signing a copy of Exhibit A; (b) such expert or consultant is not a current officer, director, or employee of a Party or of a competitor of a Party, nor anticipated at the time of retention to become an officer, director or employee of a Party or of a competitor of a Party; (c) such expert or consultant accesses the materials in the United States only, and does not transport them to or access them from any foreign jurisdiction, and (d) no unresolved objections to such disclosure exist after proper notice has been given to all Parties as set forth in Paragraph 13 below. Without the express prior written consent of the Defendant that produced the Protected Material, no expert or consultant retained by a Defendant in this matter shall have access to "CONFIDENTIAL – ATTORNEYS' EYES ONLY" Discovery Material produced by another Defendant in this matter;

Plaintiff's Statement:

Defendants' proposal introduces needless, additional restrictions already covered by other provisions in the Protective Order. Under Paragraph 13, before outside experts or consultants can even access Confidential material, they must: (1) be disclosed to the Producing Party, (2)

overcome any objections by the Producing Party, *and* (3) sign and agree to be bound by the provisions of the Protective Order by signing a copy of Exhibit A. Defendants' concerns regarding individuals who access Confidential material can and will be vetted through the Notice of Disclosure process as described in Paragraph 13.

To reflect the reality that many experts rely on supporting teams, ContentGuard proposes inclusion of "supporting personnel" as individuals who can access Confidential material, assuming other provisions of the Protective Order are met.

Defendants' Statement:

The section presents two disputes that recur in several other sections of the protective order, including Sections 6(c); 9(d)(i); 9(d)(ii); 10(c)(i). The recurring disputes include (a) whether experts (or counsel or supporting personnel) may use Protected Material for competitive gain, and (b) whether Protected Material may be taken outside the United States.

Competitive Use by Experts: Defendants' proposal limits disclosure of their most sensitive materials to people who will not be competitive decisions makers, while Plaintiff provides no limitation on whether Protected Material may be provided to competitive decision makers. Courts recognize that access to discovery can be denied to "competitive decision makers" who may inadvertently use the material for inappropriate purposes. *U.S. Steel Corp. v. United States*, 730 F.2d 1465, 1468 (Fed. Cir. 1984); *ST Sales Tech Holdings, LLC v. Daimler Chrysler Co*, No. 6:07-cv-346, 2008 WL 5634214, at *7 (E.D. Tex. Mar. 14, 2008). Confidential materials should not be disclosed to experts (or supporting personnel or counsel) who are involved in competitive decision-making activities, such as patent acquisition. An individual should not be able to study highly confidential materials, and then advise Plaintiff (or other clients) on patent monetization or acquisition strategies, for example. The risk is too great

that even a well-intentioned individual will not be able to segregate and suppress in his or her mind what was learned from studying Defendants' highly confidential internal documents when advising Plaintiff or other clients on competitive issues. *See In re Deutsche Bank*, 605 F.3d at 1378 (quoting *FTC v. Exxon Corp.*, 636 F.2d 1336, 1350 (D.C. Cir. 1980)).[11]

One of the related and recurring disputes between the parties is whether to include repeated loopholes in the limits on disclosure of Protected Material though "supporting personnel" assisting Plaintiff's disclosed experts. Such supporting personnel are likely to be trained in the technologies they are reviewing and so are a competitive threat. As a result, the limits that apply to disclosed experts should not open the door to legions of unnamed supporting personnel.

Exporting Protected Material: Defendants' position concerning Plaintiff's proposal to export Defendants' Protected Material is set forth in Section 6(c), above.

[11] *See also* Section 9(d)(i), below.

6. Paragraph 9(d)(i) – Discovery Material Designated as "Confidential – Outside Attorneys' Eyes Only"

Plaintiff's Proposal	Defendants' Proposal
Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY" may be disclosed only to: (i) The Receiving Party's Outside Counsel, and such Outside Counsel's paralegals and staff, and any copying or clerical litigation support services working at the direction of such counsel, paralegals, and staff;	Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY" may be disclosed only to: (i) The Receiving Party's Outside Counsel, provided that such Outside Counsel is not involved in competitive decision-making, as defined by *U.S. Steel v. United States*, 730 F.2d 1465, 1468 n.3 (Fed. Cir. 1984), on behalf of a Party or a competitor of a Party, and such Outside Counsel's paralegals and staff, and any copying or clerical litigation support services working at the direction of such counsel, paralegals, and staff;

Plaintiff's Statement:

ContentGuard respectfully opposes the additional language proposed by Defendants for two reasons. First, Defendants' proposal deviates from the Model Protective Order. Second, the proposal is unduly restrictive and unnecessary. Again, the Protective Order already includes (1) a provision that makes clear that Protected Material produced in this case "shall be used by a Receiving Party solely for this case, and shall not be used directly or indirectly for any other purpose whatsoever"; (2) a prosecution bar that provides protection in the patent prosecution context; (3) a provision that prohibits counsel from disclosing "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY" to its clients. Defendants' proposal to apply the "competitive

decision-maker" limitation[12] to outside counsel in *every* context and with respect to *any* client is unnecessary, as well as unduly burdensome.

Defendants' Statement:

Defendants' position concerning Plaintiffs' proposal to share Defendants' Protected Materials with competitive decision makers is set forth in Section 8(c)(iii), above.

Plaintiff's proposal in this section completely eliminates restrictions on counsel's competitive decision making, such as patent acquisition practices, within the scope of the technology relevant to this case and the Defendants production of trade secret, Protected Material. Choosing what patents to buy to be able to extract licensing revenues implicates the same competitive-decision-making concerns that justify the prosecution bar in Section 6(b). Plaintiff's proposed language expressly allows counsel that advises Plaintiff or other clients on acquisition of patents to have access to confidential material relating to, for example, Apple iTunes or the Amazon Kindle Fire. Allowing counsel who advises clients on patent acquisitions to have access to confidential information about the Defendants' products would be highly injurious and prejudicial. Nor should counsel be permitted to advise other clients on patent acquisition in light of information they learned through the production of the Defendants' confidential information.

[12] In *U.S. Steel Corp. v. United States*, the Federal Circuit addressed whether a court *may* limit "competitive decision-makers" from access to sensitive information based on the risk of their inadvertently disclosing protected information as a result of their "long and intimate relationships and activities with" the parties they represent in that litigation matter. 730 F.2d 1465, 1467-68 (Fed. Cir. 1984). *U.S. Steel* counsels against the application of categorical protective orders in favor of "specific provisions . . . developed in light of the particular counsel's relationship and activities." *Id.* Notably, *U.S. Steel* ultimately reversed a decision denying access to an in-house lawyer because denying access "would create an extreme and unnecessary hardship." *Id.* at 1468. In *In re Deutsche Bank Trust*, the Federal Circuit added that "[t]he concern over inadvertent disclosure manifests itself in patent infringement cases when trial counsel also represent the same client in prosecuting patent applications before the PTO." 605 F.3d 1373, 1378 (Fed. Cir. 2010).

7. Paragraph 9(d)(ii) – Discovery Material Designated as "Confidential – Outside Attorneys' Eyes Only"

Plaintiff's Proposal	Defendants' Proposal
Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY" may be disclosed only to: (ii) Any outside expert or consultant retained by the Receiving Party to assist in this action and supporting personnel, provided that disclosure is only to the extent necessary to perform such work; and provided that: (a) such expert or consultant has agreed to be bound by the provisions of the Protective Order by signing a copy of Exhibit A; and (b) no unresolved objections to such disclosure exist after proper notice has been given to all Parties as set forth in Paragraph 13 below. Without the express prior written consent of the Defendant that produced the Protected Material, no expert or consultant retained by a Defendant in this matter shall have access to "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY" Discovery Material produced by another Defendant in this matter;	Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY" may be disclosed only to: (ii) Any outside expert or consultant retained by the Receiving Party to assist in this action, provided that disclosure is only to the extent necessary to perform such work; and provided that: (a) such expert or consultant has agreed to be bound by the provisions of the Protective Order by signing a copy of Exhibit A; (b) such expert or consultant is not a current officer, director, or employee of a Party or of a competitor of a Party, nor anticipated at the time of retention to become an officer, director, or employee of a Party or of a competitor of a Party; (c) such expert or consultant is not involved in competitive decision-making, as defined by *U.S. Steel v. United States*, 730 F.2d 1465, 1468 n.3 (Fed. Cir. 1984), on behalf of a Party or a competitor of a Party; (d) such expert or consultant accesses the materials in the United States only, and does not transport them to or access them from any foreign jurisdiction; and (e) no unresolved objections to such disclosure exist after proper notice has been given to all Parties as set forth in Paragraph 13**Error! Reference source not found.** below. Without the express prior written consent of the Defendant that produced the Protected Material, no expert or consultant retained by a Defendant in this matter shall have access to "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY" Discovery Material produced by another Defendant in this matter;

Plaintiff's Statement:

Plaintiff's statement is set forth in Disputed Provisions 5 and 6 above.

Defendants' Statement:

Defendants' position concerning Plaintiffs' proposal to share Defendants' Protected Materials with competitive decision makers is set forth in Section 8(c)(iii) and 9(d)(i), above. Defendants' position concerning Plaintiff's proposal to export Defendants' Protected Material is set forth in Section 6(c), above.

8. Paragraph 10(c)(i) - Discovery Material Designated as "Confidential – Outside Attorneys' Eyes Only – Source Code"

Plaintiff's Proposal	Defendants' Proposal
Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be subject to the provisions set forth in Paragraph **Error! Reference source not found.** below, and may be disclosed, subject to Paragraph **Error! Reference source not found.** below, solely to: (i) The Receiving Party's Outside Counsel and such Outside Counsel's paralegals and staff, and any copying or clerical litigation support services working at the direction of such counsel, paralegals, and staff.	Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be subject to the provisions set forth in Paragraph **Error! Reference source not found.** below, and may be disclosed, subject to Paragraph **Error! Reference source not found.** below, solely to: (i) The Receiving Party's Outside Counsel, provided that such Outside Counsel is not involved in competitive decision-making, as defined by *U.S. Steel v. United States*, 730 F.2d 1465, 1468 n.3 (Fed. Cir. 1984), on behalf of a Party or a competitor of a Party, and such Outside Counsel's paralegals and staff, and any copying or clerical litigation support services working at the direction of such counsel, paralegals, and staff;

Plaintiff's Statement:

Plaintiff's statement is set forth in Disputed Provision 6 above.

Defendants' Statement:

Defendants' position concerning Plaintiffs' proposal to share Defendants' Protected Materials with competitive decision makers is set forth in Sections 8(c)(iii) and 9(d)(i), above.

9. Paragraph 10(c)(ii) - Discovery Material Designated as "Confidential – Outside Attorneys' Eyes Only – Source Code"

Plaintiff's Proposal	Defendants' Proposal
Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be subject to the provisions set forth in Paragraph **Error! Reference source not found.** below, and may be disclosed, subject to Paragraph **Error! Reference source not found.** below, solely to: . . . (ii) Up to <u>five (5)</u> outside experts or consultants[13] retained by the Receiving Party to review each disclosing Party's Source Code, provided that disclosure is only to the extent necessary to perform such work; and provided that: (a) such expert or consultant has agreed to be bound by the provisions of the Protective Order by signing a copy of Exhibit A; (b) no unresolved objections to such disclosure exist after proper notice has been given to all Parties as set forth in Paragraph **Error! Reference source not found.** below; and (c) such expert is specifically identified as eligible to access Source Code. Without the express prior written consent of the Defendant that produced the Protected Material, no expert or consultant retained by a Defendant in this matter shall have access to "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" Discovery Material produced by another Defendant in this matter;	Unless otherwise ordered by the Court, Discovery Material designated as "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be subject to the provisions set forth in Paragraph **Error! Reference source not found.** below, and may be disclosed, subject to Paragraph **Error! Reference source not found.** below, solely to: . . . (ii) Up to <u>four (4)</u> outside experts or consultants[14] retained by the Receiving Party to review each disclosing Party's Source Code, provided that disclosure is only to the extent necessary to perform such work; and provided that: (a) such expert or consultant has agreed to be bound by the provisions of the Protective Order by signing a copy of Exhibit A; (b) no unresolved objections to such disclosure exist after proper notice has been given to all Parties as set forth in Paragraph **Error! Reference source not found.** below; and (c) such expert is specifically identified as eligible to access Source Code. Without the express prior written consent of the Defendant that produced the Protected Material, no expert or consultant retained by a Defendant in this matter shall have access to "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" Discovery Material produced by another Defendant in this matter;

[13] For the purposes of this paragraph, an outside consultant or expert is defined to include the outside consultant's or expert's direct reports and other support personnel, such that the disclosure to a consultant or expert who employs others within his or her firm to help in his or her analysis shall count as a disclosure to a single consultant or expert.

[14] No footnote.

Plaintiff's Statement:

This litigation involves twelve defendants and more than 500 accused products using DRM. The source code productions in this case are likely to be extremely large and include many different versions. Defendants' proposal that this gargantuan task be performed by only four individuals is woefully unrealistic. The Court should allow ContentGuard to use five experts. In addition, ContentGuard's experts and consultants require direct reports and support personnel to assist in the source code review and in the preparation of claim charts pursuant to P.R. 3-1(g). ContentGuard thus proposes the inclusion of footnote 2, which is verbatim from page 6 of the Court's Model Protective Order.

Defendants' Statement:

Plaintiff's repeated efforts to open the door to Protected source code beyond clearly disclosed counsel and experts renders many of the proposed protections illusory. Plaintiff's proposal would permit 5 experts per Defendant, plus any number of "direct reports and support personnel" full access to Defendants' most highly protected information. In contrast, Defendants do not propose that Plaintiff may only have four experts in total for this case. Rather, Defendants propose that Plaintiff may designate up to four experts with source code access *for each Defendant.* This limit appropriately balances the needs of this case against the interests of the Defendants and the public in maintaining the security of the accused DRM technologies.

Courts have repeatedly recognized that source code is highly sensitive, highly valuable and should be protected accordingly. *See e.g., Geotag, Inc. v Frontier Communs. Corp.*, 2013 U.S. Dist. LEXIS 25774 at *261 (E.D. Tex. Jan. 7, 2013) (explaining that additional protections were needed for source code because of its "highly confidential nature" and that the interests of

protecting the code far outweighed the conveniences that plaintiff sought in accessing it); *Evolutionary Intelligence, LLC v. Apple, Inc.*, 6:12-cv-00783, slip op. at 9 (E.D. Tex. Aug. 27, 2013) (considering the sensitive nature of Twitter's California-based source code in ordering transfer to the Northern District of California). For example, as one of the largest and most highly publicized companies in the world, Apple's trade secrets are extremely sought after. Apple's competitors and the "tech blogosphere" (i.e., the community publishing the latest technology releases, leaks, and rumors) daily search for and broadcast virtually every scrap of activity they can learn about Apple's products and activities. *See e.g.*, http://appleinsider.com/articles/13/06/19/leaked-schematics-reveal-what-case-makers-expect-apples-low-cost-iphone-iphone-5s-will-look-like. If Apple's most sensitive trade secrets—its source code—were to be disseminated in any manner, even inadvertently, Apple would face potentially devastating competitive harm. *See e.g.*, Declaration of Payam Mirrashidi, at ¶ 5 (explaining that iTunes Store source code is a highly confidential and valuable proprietary trade secret, a core asset of Apple's business); Declaration of Beth Kellermann ¶ 5.

Furthermore, the confidentiality of Apple's source code helps keep products secure from hacking and other threats, such as viruses. For example, the security of sensitive customer information, such as credit cards numbers and purchase histories, would be compromised by improper access to iTunes Store source code because it would inform would-be attackers exactly how iTunes manages and transmits such information. Any breach of security would result in grave and irreparable harm that could affect not only Apple, but millions of consumers.

Despite the acknowledged importance of protecting source code, Plaintiff seeks to significantly weaken or eliminate the protections provided for source code. Plaintiff's proposals: (1) Relaxes and eliminates restrictions on printing and copying source code, (2) Removes

restrictions on the producing party's ability to object to providing printed copies of the source code, (3) Removes restrictions on transporting the source code, (4) Substantially expands the number of people with access to the code, (5) Removes restrictions on recording and transmitting devices into the source code room, (6) Requires unreasonable and unworkable notice periods for ensuring a secure and efficient source code inspection. Each of these proposals individually, and especially when viewed together, dramatically increase the risk that at least some portion of the highly confidential source code will be disseminated and used outside of this litigation.

The Defendants' proposed source code provisions are not only reasonable, but are consistent with the highly controlled source code access policies. For example, Apple maintains code regarding its methods and algorithms for iTunes on servers entirely hidden from the public. Mirrashidi Decl. ¶ 7. Further, the iTunes Store source code is provided the highest level of protection and security within Apple – physical access is limited to select groups of authorized Apple employees who are only even granted access to portions of the code on a need-to-know basis. Mirrashidi Decl. ¶ 6. Access is strictly limited to employees directly involved in software development, management, and security. Mirrashidi Decl. ¶ 6. Indeed, Apple does not even allow its own experts during litigation to have electronic or hard copies of its source code. Kellermann Decl. ¶ 6. The protections Defendants seek with respect to Plaintiff's access, use, printing, and transport of source code are narrowly tailored to ensure protection of the source code and identify any breaches at the earliest possible time.

In this Section 10(c)(ii), Defendants object to provisions that would grant source code access to an unlimited and unidentified group of "direct reports" and "support personnel" for Plaintiff's experts. The trade secret status of the source code is hard enough to maintain, and substantially expanding the number of persons with knowledge unnecessarily and unreasonably

increases the risk that source code will be leaked. In this case, the source code at issue primarily concerns encryption, which only increases the risk to both Defendants and the public in the event such a leak leads to a hack. Simply put, Plaintiffs interests in throwing innumerable unnamed, undisclosed consultants at the source code is greatly outweighed by the risk of harm to both Defendants and the public. *See, e.g.*, This Court's Sample Protective Order for Patent Cases ¶ 5(e) (requiring advance disclosure of the identity and other information for all outside consultants and experts).

10. Paragraph 11(b) - Disclosure and Review of Source Code

Plaintiff's Proposal	Defendants' Proposal
Prior to the first inspection of any requested Source Code, the Receiving Party shall provide twenty-one (21) days' notice of the Source Code that it wishes to inspect and shall meet and confer with the Producing Party in good faith to determine a date for first inspection. The Receiving Party shall provide two (2) days' notice prior to any additional inspections of previously produced code.	Prior to the first inspection of any requested Source Code, the Receiving Party shall provide twenty-one (21) days' notice of the Source Code that it wishes to inspect and shall meet and confer with the Producing Party in good faith to determine a date for first inspection. The Receiving Party shall provide ten (10) days' notice prior to any additional inspections of previously produced code.

Plaintiff's Statement:

ContentGuard respectfully submits that two days' notice is sufficient to schedule additional Source Code inspections of previously-produced code. Defendants' proposal for ten days' notice is unreasonable and unduly burdensome. The agreed language in the Protective Order provides for twenty-one days' notice for the first source code inspection. Any subsequent inspections of the source code should not require a lengthy notice period because the source code will already be available and set up for review. ContentGuard's experts and consultants cannot always plan their travel and work schedules to provide for ten days' notice prior to subsequent inspections.

Defendants' Statement:

Plaintiff's proposed two day notice provision ignores the time and effort required to set up a secure source code inspection site and would give Plaintiff a powerful strategic advantage. As a simple matter of logistics, Defendants cannot guarantee that sufficient personnel will be available and on site to set up a secure source code review room with only two days' notice. Defendants therefore request 10 days' notice. Additionally, a two day notice provision effectively requires the relevant personnel and outside counsel for the Producing Party to drop

everything to address the additional inspection request. This strategic tool could be abused around the time of depositions, briefing and other case-related events. The more prudent course is to require ten days' notice, which still obligates the Producing Party to act quickly, but will not jeopardize business or legal interests and will preclude potential abuse of additional inspections.

Plaintiff has not articulated any reason why it cannot provide more notice to the Defendants of its requested inspections. Given the highly sensitive nature of the source code, and internal procedures required by the Defendants to release that source code for these kinds of inspections, additional time is justified—particularly given that Plaintiff has not identified any problem or impediment in allowing Defendants that additional time.

Defendants are willing to cooperate with Plaintiff to attempt to meet any requests for inspection less than 10 days before any additional inspection, to the extent practicable. However, Defendants cannot guarantee that they will be able to meet shorter time periods, and do not want to agree to highly restrictive time limits that could potentially leave Defendants in violation of the protective order if it is not possible to meet those limits.

11. Paragraph 11(c)(i) - Disclosure and Review of Source Code

Plaintiff's Proposal	Defendants' Proposal
Source Code that is designated "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be produced for inspection and review subject to the following provisions, unless otherwise agreed by the Producing Party: (i) All Source Code shall be made available by the Producing Party to the Receiving Party's outside counsel and/or experts in a secure room on five (5) secured, password-protected computers without Internet access or network access to other computers other than to a computer hosting the Source Code material and on which all access ports have been disabled, as necessary and appropriate to prevent and protect against any unauthorized copying, transmission, removal or other transfer of any Source Code outside or away from the computers on which the Source Code is provided for inspection (the "Source Code Computers" in the "Source Code Review Room"). The Producing Party shall install tools that are sufficient for viewing and searching the code produced, on the platform produced, if such tools exist and are presently used in the ordinary course of the Producing Party's business. The Receiving Party's outside counsel and/or experts may request that commercially available software tools for viewing and searching Source Code be installed on the secured computers, provided, however, that (a) the Receiving Party possesses an appropriate license to such software tools; and (b) such other software tools are reasonably necessary for the Receiving Party to perform its review of the Source Code consistent with all of the protections herein. The Receiving Party must provide the Producing Party with the licensed software tool(s) at least five (5) days in advance of the date upon which the Receiving Party wishes to have the additional software tools available for use on the Source Code Computers. The Producing Party shall provide any additionally requested Source Code material for inspection within fourteen (14) days of when it is first identified by the Receiving	Source Code that is designated "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be produced for inspection and review subject to the following provisions, unless otherwise agreed by the Producing Party: (i) All Source Code shall be made available by the Producing Party to the Receiving Party's outside counsel and/or experts in a secure room on secured, password-protected computers without Internet access or network access to other computers other than to a computer hosting the Source Code material and on which all access ports have been disabled, as necessary and appropriate to prevent and protect against any unauthorized copying, transmission, removal or other transfer of any Source Code outside or away from the computers on which the Source Code is provided for inspection (the "Source Code Computers" in the "Source Code Review Room"). One Source Code Computer shall be provided by Producing Party for each outside expert or consultant identified in Paragraph 10(c)(ii). The Producing Party shall install tools that are sufficient for viewing and searching the code produced, on the platform produced, if such tools exist and are presently used in the ordinary course of the Producing Party's business. The Receiving Party's outside counsel and/or experts may request that commercially available software tools for viewing and searching Source Code be installed on the secured computers, provided, however, that (a) the Receiving Party possesses an appropriate license to such software tools; and (b) the Producing Party approves such software tools which approval shall not be unreasonably

Party. The parties agree that the following software tools are pre-approved: • SlickEdit (http://www.slickedit.com) • Understand (http://www.scitools.com) • Beyond Compare (http://www.scootersoftware.com) • Acrobat (http://get.adobe.com/reader) • Cygwin (http://www.cygwin.com) • Edit Pad Lite (http://www.editpadlite.com) • EditPadPro (http://www.editpadpro.com/) • Xcode (https://developer.apple.com/xcode) • TextWrangler (http://www.barebones.com/products/textwrangler) • Eclipse (http://www.eclipse.org) • Notepad++ (http://notepad-plus-plus.org/download/v6.4.5.html) • Windows Grep (http://www.wingrep.com/download.htm)	withheld; and (c) such other software tools are reasonably necessary for the Receiving Party to perform its review of the Source Code consistent with all of the protections herein. The Receiving Party must provide the Producing Party with the licensed software tool(s) at least ten (10) days in advance of the date upon which the Receiving Party wishes to have the additional software tools available for use on the Source Code Computers. The Producing Party shall provide any additionally requested Source Code material for inspection within twenty-one (21) days of when it is first identified by the Receiving Party.

Plaintiff's Statement:

With respect to the number of computers made available for source code review, ContentGuard respectfully submits that each expert should be provided a computer. Further, as explained above (*see* Disputed Provision 9), ContentGuard respectfully submits that at leave five experts (and supporting personnel) are needed to conduct source code review given the large number of products and source code versions anticipated for each Defendant, and the pace of the litigation.

The five days' notice provision is reasonable because ContentGuard has already told Defendants the type of software tools ContentGuard's experts may use to conduct the review. ContentGuard has identified the pre-approved software tools that are commonly used during source code reviews and which its experts have requested in order to efficiently conduct the source code review.

Defendants' Statement:

Defendants' overview concerning Plaintiffs' proposals that substantially weaken the protections for source code is set forth in Section 10(c)(ii), above.

The parties have discussed twelve software packages that the plaintiff can provide for installation. Most of the packages are non-standard in the law firm setting, and may require significant time for Defendants' technical support staff to review, install, and troubleshoot. Not all the tools are useable with all source code, and several are redundant. Plaintiff also has the option of requesting that an unlisted software package be installed. Defendants request adequate time to ensure the tools can be loaded on the review computers, and verify that the tools operate correctly. As in number of other sections, Plaintiff's timing demands are entirely unnecessary and would impose substantial burdens on each Defendant.

Defendants also have reasonably tied the number of review computers to the number of experts. Plaintiff's proposal would unnecessarily require each Defendant to set up 5 review computers even if only one, two, three or four experts will be present for the review.

12. Paragraph 11(c) - Disclosure and Review of Source Code

Plaintiff's Proposal	Defendants' Proposal
No provision	No recordable media or recordable devices, including without limitation sound recorders, computers, cellular telephones, peripheral equipment, cameras, CDs, DVDs, or drives of any kind, shall be permitted into the Source Code Review Room. All persons entering the secure room containing the Source Code must agree to submit to reasonable security measures to insure they are not carrying any prohibited items before they will be given access to the secure room.

Plaintiff's Statement:

ContentGuard respectfully opposes the additional language proposed by Defendants for two reasons. First, Defendants' proposal deviates from the Model Protective Order. Second, ContentGuard's experts and consultants may require access to their computers and telephones in the source code review room to effectively conduct the inspection. Despite limitations to a standalone computer and visual monitoring, Defendants also demand that ContentGuard not use any electronic devices during its source code review. This prohibition unfairly hinders ContentGuard's ability to make use of computers or other technology to efficiently take notes and update claim charts pursuant to P.R. 3-1(g). In addition, some portions of relevant source code may be publically available on the internet. ContentGuard would obviously need the ability to compare and determine what portions of Defendants' code are publically available during its review. ContentGuard would need electronic copies of publically available source code to search and compare to the source code provided during the review. This would also promote an efficient review and selection of material portions for production. It is also unreasonable to limit ContentGuard to handwritten notes of source code, which would then later need to be typed into

a computer. Along the same lines, ContentGuard's code reviewers may need access to their telephones in the source code review room to consult with outside counsel or other experts. ContentGuard respectfully submits that Defendants' concerns about the potential misuse of electronic devices by ContentGuard is misplaced and exaggerated. The Protective Order contains ample safeguards against such misuse, including Defendants' absolute right to monitor ContentGuard's source code review.

Defendants' Statement:

Defendants' overview concerning Plaintiffs' proposals to substantially weaken the protections for source code is set forth in Section 10(c)(ii), above.

In this section, Defendants propose to eliminate any device capable of recording, copying or transmitting from the room where the source code is inspected. Plaintiff, by contrast, seeks to remove this restriction altogether, substantially increasing the risk that the source code can be surreptitiously copied and transmitted. Defendants' restriction on recording and transmitting devices is necessary to protect the highly sensitive source code and is entirely consistent with orders from this Court. *Geotag, Inc. v. Frontier Comms. Corp.*, 2:10-cv-265 (E.D. Tex. Jan. 8, 2013).[15] In *Geotag*, for example, this Court expressly prohibited media devices from entering the source code room, despite plaintiff's complaints about efficiency and their assurances that the rest of the protective order was sufficient protection. *Id.* at 7. Plaintiff asserts the same arguments rejected by this Court in *Geotag*, providing no basis for doing away with the restriction on media devices in the source code room. Plaintiff's hypothetical that it may locate publicly available source code does not justify the risks to Defendants' source code through

[15] The *Geotag* protective order is available in the Greenblatt Decl. at Ex. 9.

allowing network computers into the source code review room. Plaintiff may certainly bring a hard copy of such code with them to compare.

13. Paragraph 11(c)(ii) - Disclosure and Review of Source Code

Plaintiff's Proposal	Defendants' Proposal
Source Code that is designated "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be produced for inspection and review subject to the following provisions, unless otherwise agreed by the Producing Party: . . . (ii) The Receiving Party's outside counsel and/or experts shall be entitled to take notes relating to the Source Code but may not copy the Source Code into the notes and may not take notes electronically on the Source Code Computer itself.	Source Code that is designated "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be produced for inspection and review subject to the following provisions, unless otherwise agreed by the Producing Party: . . . (ii) The Receiving Party's outside counsel and/or experts shall be entitled to take notes relating to the Source Code but may not copy the Source Code into the notes and may not take notes electronically on the Source Code Computer itself or any other computer.

Plaintiff's Statement:

This is dispute is related to Disputed Provision 12 above. ContentGuard submits that this additional provision is unnecessary. The agreed language in the Protective Order already allows experts and consultants to take notes relating to the Source Code. Any restrictions on how notes should be taken are completely unreasonable, impracticable, and archaic.

Defendants' Statement:

Defendants' overview concerning Plaintiffs' proposals to substantially weaken the protections for source code is set forth in Section 10(c)(ii), above. Defendants' position on allowing recording and computing devices into the source code review room is set forth in Section 11(c) above. Each Defendant is willing to provide supervised access to a computer that lacks any photo or video capture ability, and lacks any network connection, for purposes of note

taking, with such notes provided at the conclusion of each day of the inspection. Notes will be provided in either hard copy or on a USB drive, at the option of the producing party.

14. Paragraph 11(c)(iv) - Disclosure and Review of Source Code

Plaintiff's Proposal	Defendants' Proposal
Source Code that is designated "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be produced for inspection and review subject to the following provisions, unless otherwise agreed by the Producing Party: . . . (iv) No person shall copy, e-mail, transmit, upload, download, print, photograph or otherwise duplicate any portion of the designated Source Code, except as the receiving party may request a reasonable number of pages of Source Code to be printed by the producing party, but only if and to the extent necessary for use in this action. The Receiving Party may print out no more than 10% of the source code for an accused product absent good cause. The Receiving Party shall not print Source Code in order to review blocks of Source Code elsewhere in the first instance, *i.e*., as an alternative to reviewing that Source Code electronically on the Source Code Computer, as the Parties acknowledge and agree that the purpose of the protections herein would be frustrated by printing portions of code for review and analysis elsewhere, and that printing is permitted only when necessary to prepare court filings or pleadings or other papers (including a testifying expert's expert report). Within two (2) days, the Producing Party shall provide one copy set of such pages to the Receiving Party on watermarked or colored paper bearing Bates numbers and the legend "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE". The printed pages shall constitute part of the Source Code produced by the Producing Party in this action. At the inspecting parties request, up to two additional sets (or subsets) of printed Source Code may	Source Code that is designated "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be produced for inspection and review subject to the following provisions, unless otherwise agreed by the Producing Party: . . . (iv) No person shall copy, e-mail, transmit, upload, download, print, photograph or otherwise duplicate any portion of the designated Source Code, except as the receiving party may request a reasonable number of pages of Source Code to be printed by the producing party, but only if and to the extent necessary for use in this action. Any printed portion that consists of more than forty (40) pages of a continuous block of Source Code shall be presumed to be excessive, and the burden shall be on the Receiving Party to demonstrate the need for such a printed copy. The Receiving Party may print out no more than the lesser of 200 pages total or 10% of the reviewed lines of source code. The Receiving Party shall not print Source Code in order to review blocks of Source Code elsewhere in the first instance, *i.e*., as an alternative to reviewing that Source Code electronically on the Source Code Computer, as the Parties acknowledge and agree that the purpose of the protections herein would be frustrated by printing portions of code for review and analysis elsewhere, and that printing is permitted only when necessary to prepare court filings or pleadings or other papers (including a testifying expert's expert report). Within ten (10) days, the Producing Party shall either (i) provide one copy set of such pages to the Receiving Party on watermarked or colored paper bearing Bates numbers and the legend "CONFIDENTIAL – OUTSIDE

be requested and provided by the producing party in a timely fashion. The Receiving Party shall be permitted to make a reasonable number of photocopies of the printed Source Code, all of which shall be designated and clearly labeled "CONFIDENTIAL – OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE," and the Receiving Party shall maintain a log of all such files that are photocopied.	ATTORNEYS' EYES ONLY - SOURCE CODE" or (ii) inform the Requesting Party that it objects that the printed portions are excessive and/or not done for a permitted purpose. If, after meeting and conferring, the Producing Party and the Receiving Party cannot resolve the objection, the Receiving Party shall be entitled to seek a Court resolution of whether the printed Source Code in question is narrowly tailored and was printed for a permitted purpose. The burden shall be on the Receiving Party to demonstrate that such printed portions are no more than is reasonably necessary for a permitted purpose and not merely printed for the purposes of review and analysis elsewhere. Contested Source Code print outs need not be produced to the requesting party until the matter is resolved by the Court. The printed pages shall constitute part of the Source Code produced by the Producing Party in this action. At the inspecting parties request, up to two additional sets (or subsets) of printed Source Code may be requested and provided by the producing party in a timely fashion.

Plaintiff's Statement:

ContentGuard respectfully opposes the additional language proposed by Defendants for two reasons. First, Defendants' proposal deviates from the Model Protective Order. Second, Defendants' proposal introduces unreasonable, completely arbitrary, and highly limiting restrictions related to the printing and copying of source code.

With respect to the printing of source code, Defendants seek to limit ContentGuard to no more than the lesser of 200 pages total or 10% of the reviewed pages and no more than 40 continuous pages. On their face, these numbers are absurd. ContentGuard has accused more than 500 devices, each of which is likely to run multiple version of source code. Defendants' proposal, however, would not even allow ContentGuard to print one page of source code per

accused product. Imposing such limitations is particularly egregious given that (1) Defendants have rejected ContentGuard's proposal for a representative model stipulation, which would have greatly reduced the amount of source code Defendants are required to produce; and (2) Defendants have not yet produced any source code, such that it is impossible to know how large Defendants' productions will be. ContentGuard respectfully requests that the Court reject Defendants' proposal and instead order that the parties live by the tried-and-true "reasonableness" standard and absent good cause no more than 10% of the source code for the accused product. ContentGuard's "no more than 10%" approach was already endorsed by Chief Judge Leonard Davis in the Supplemental Protective Order entered under Docket Number 191 in *Wi-LAN, Inc. v. Alcatel-Lucent Corporation*, et al., 6:10-cv-00521-LED. Defendants are of course free to seek relief from the Court if they believe that ContentGuard is acting unreasonably.

Defendants' proposal would appear to altogether foreclose ContentGuard from making photocopies of produced source code. There is no basis for such a restriction. ContentGuard thus respectfully submits that the Court include the language from section 10(h) of the Court's Model Protective Order, which permits ContentGuard to make a reasonable number of photocopies of the printed Source Code.

Defendants' Statement:

Defendants' overview concerning Plaintiff's proposals to substantially weaken the protections for source code is set forth in Section 10(c)(ii), above.

In this section, Plaintiff proposes that it be permitted to print an unlimited number of pages of source code, and an unlimited number of copies of such source code. As with the number of eyeballs that review the source code, the number and extent of copies unnecessarily

and unreasonably increases the risk of leaks and hacks that would cause irreparable harm to the producing Defendant, and to the public. In contrast, the Defendants' proposal provides a procedure for reasonable printouts of source code. This proposal allows Plaintiff to print up to 40 contiguous pages of source code, with a cumulative limit of the lesser of 200 pages or 10% of reviewed lines of source code, and is consistent with protective orders issued previously by this Court. *See e.g.*, *First American Corelogic*, No. 2:10-cv-132, at ¶ 24 ("No more than 10% or 500 pages (whichever is smaller) of the total source code for any software release may be in printed form at any one time, and all printed source code shall be logged by the recipient").[16] In contrast, Plaintiff's demand for 10% of all source code for each product whether it was reviewed effectively means that Plaintiff could demand print outs of all reviewed code because the code for the product will likely be more extensive than the code relevant to Plaintiff's claims. Defendants' proposal also provides for a reasonable time for review and production of any copy permitted by the protective order. Plaintiff will not be prejudiced by the 10-day period, while Plaintiff's 2-day provision does not permit adequate time.

[16] The *First American* protective order is available in the Greenblatt Decl. at Ex. 10.

15. Paragraph 11(c)(viii) - Disclosure and Review of Source Code

Plaintiff's Proposal	Defendants' Proposal
Any paper copies designated "CONFIDENTIAL - OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be stored or viewed only at (i) the offices of outside counsel for the receiving party, (ii) the offices of outside experts or consultants who have been approved to access Source Code; (iii) the site where any deposition is taken (iv) the Court; or (v) any intermediate location necessary to transport the information to a hearing, trial or deposition. The Receiving Party's outside counsel of record and any person receiving a copy of any Source Code shall maintain and store any paper copies of the Source Code at their offices in a manner that prevents duplication of or unauthorized access to the Source Code, including, without limitation, storing the Source Code in a locked room or cabinet at all times when it is not in use.	Any paper copies designated "CONFIDENTIAL - OUTSIDE ATTORNEYS' EYES ONLY - SOURCE CODE" shall be stored or viewed only at (i) the offices of outside counsel for the receiving party, (ii) the offices of outside experts or consultants who have been approved to access Source Code; (iii) the site where any deposition is taken (iv) the Court; or (v) any intermediate location necessary to transport the information to a hearing, trial or deposition. The Receiving Party's outside counsel of record and any person receiving a copy of any Source Code shall maintain and store any paper copies of the Source Code at their offices in a manner that prevents duplication of or unauthorized access to the Source Code, including, without limitation, storing the Source Code in a locked room or cabinet at all times when it is not in use. No more than a total of ten (10) individuals identified by the Receiving Party shall have access to the printed portions of each respective Defendants' Source Code (except insofar as such code appears in any court filing or expert report).

Plaintiff's Statement:

ContentGuard respectfully opposes the additional language proposed by Defendants for two reasons. First, Defendants' proposal deviates from the Model Protective Order. Second Defendants' proposed language would arbitrarily limit access to the printed source code to far too few individuals. Given the size of the team required to handle a case involving 12 defendants and more than 500 accused products, and the pace of the litigation, ContentGuard's counsel alone requires more than 10 individuals to have access to the printed source code. Given that experts and consultants will also need to access source code to prepare expert reports, it is

not reasonable or feasible to put an arbitrary limit on the number of individuals who have access to the printed source code.

Defendants' Statement:

Defendants' overview concerning Plaintiff's proposals to substantially weaken the protections for source code, including the reasons for Defendants' objection to Plaintiff's proposal that unlimited numbers of "direct reports" or "supporting personnel" have access to source code, is set forth in Section 10(c)(ii), above. In summary, limiting access to a set number of identified individuals for each Defendant provides Plaintiff with the access it needs for this case while helping to ensure that encryption technologies are not hacked as the result of a preventable leak. Careful access controls must be maintained to prevent leaks, and in the event of any leak, so that the source of a leak can be quickly identified and further harm prevented.

16. Paragraph 11(x) - Disclosure and Review of Source Code

Plaintiff's Proposal	Defendants' Proposal
For depositions, upon request by the Receiving Party, the Producing Party shall bring a monitor and computer including the Source Code as it was produced on the Source Code Computers. Copies of Source Code that are marked as deposition exhibits shall not be provided to the Court Reporter or attached to deposition transcripts; rather, the deposition record will identify the exhibit by its production numbers. All paper copies of Source Code brought to the deposition shall remain with the Producing Counsel's outside counsel for secure destruction in a timely manner following the deposition	For depositions, the Receiving Party shall not bring copies of any printed Source Code without the Producing Party's prior written consent. Rather, at least ten (10) days before the date of the deposition, the Receiving Party shall notify the Producing Party about the specific portions of Source Code it wishes to use at the deposition. At the option of the Producing Party, the requested specific portions of Source Code will be provided at the deposition either in triplicate hard copy or on a monitor and computer. If the Producing Party opts to provide the specific portions of Source Code for the deposition on a monitor and computer, such deposition shall proceed at a location where the Producing Party makes Source Code available for the deposition. To the extent copies of Source Code are made during the deposition, or the Producing Party has agreed to allow portions of its Source Code be printed and copied in advance for use at the deposition, that are marked as deposition exhibits, such Source Code exhibits shall not be provided to the Court Reporter or attached to deposition transcripts; rather, the deposition record will identify the exhibit by its production numbers. All paper copies of Source Code shall remain with the Producing Counsel's outside counsel for secure destruction in a timely manner following the deposition.

Plaintiff's Statement:

ContentGuard respectfully opposes the additional language proposed by Defendants for two reasons. First, Defendants' proposal deviates from the Model Protective Order. Second Defendants' proposal introduces needless, involved logistics related to the use of source code during depositions. The protections afforded by the other provisions of the Protective Order are

sufficient to ensure that source code is maintained in confidence, and this provision is unnecessary. Defendants' proposed language saddles ContentGuard with the unnecessary burden of solidifying and disclosing the selection of source code it will use at a deposition ten days ahead of time. This is unfair, unworkable, and unnecessary, and would force ContentGuard to disclose its attorney strategy in advance of the deposition by the selection of source code well before the deposition. In addition, the pace of litigation does not allow for such clairvoyance. And under Defendants' proposed language, source code made available to ContentGuard less than ten days before a deposition would not be able to be introduced at the deposition.

Defendants' Statement:

The parties have two disputes with respect to Paragraph 11(x): (1) whether the Receiving Party or the Producing Party will provide the printed source code to be used during a deposition; and (2) whether a computer including the source code must be provided upon the Receiving Party's request. Defendants' overview concerning Plaintiff's proposals to substantially weaken the protections for source code is set forth in Section 10(c)(ii), above.

Printed Source Code: Defendants' proposal provides that the Producing Party will have the option to provide printed copies of previously-printed portions of source code at depositions or to provide those portions on a monitor and computer, and therefore the Receiving Party need not bring printed copies of the source code to the deposition. Defendants' proposal does not limit the Receiving Party's ability to use the source code during the deposition. Instead, it merely recognizes that source code is highly sensitive and highly valuable. *See e.g., Geotag, Inc. v Frontier Communs. Corp.*, 2013 U.S. Dist. LEXIS 25774 at *261 (E.D. Tex. Jan. 7, 2013) (explaining that additional protections were needed for source code because of its "highly confidential nature" and that the interests of protecting the code far outweighed the conveniences

that plaintiff sought in accessing it); *Evolutionary Intelligence, LLC v. Apple, Inc.*, 6:12-cv-00783, slip op. at 9 (E.D. Tex. Aug. 27, 2013) (considering the sensitive nature of Twitter's California-based source code in ordering transfer to the Northern District of California).

There is a large disparity between the Producing Party's interest in safeguarding its own source code, and the Receiving Party's interest in safeguarding that source code while in transit to a deposition. Given that disparity, it makes sense that the Producing Party control and protect the source code. Previous protective orders issued by this Court have recognized this disparity and granted even greater protection to the Producing Party. *See, e.g., Lodsys Group, LLC v. Dr. Pepper Snapple Group, Inc.*, 2:13-cv-00058, at 8 (requiring the Receiving Party to notify the Producing Party about specific portions of source code it wishes to use at the deposition, and the Producing Party to bring printed copies of those portions to the deposition). Indeed, the Plaintiff in the *Lodsys* case recognized that the provision would not impede its ability to conduct depositions, and therefore agreed to a more restrictive provision than the one requested by Defendants.

The Defendants' proposal does not in any way prejudice or impede the ability of the Receiving Party to conduct depositions. It is narrowly tailored to allow depositions to proceed while ensuring that the highly confidential source code is properly protected.

Source Code Computer: Defendants' proposal provides the Producing Party the option of providing printed copies or providing a computer with the source code at the location where the source code was produced. This will allow a Producing Party to provide a source code computer instead of printed copies of the source code when the deposition is held at the location where the source code was produced for inspection, and if the Producing Party believes that it will provide better protection for the source code.

Plaintiff's proposal for the use of a source code computer does not replace the provision of printed copies of the source code. Instead, the source code computer in Plaintiff's proposal apparently supplements the printed source code, and therefore would pose an even greater risk to the Producing Party's source code. In addition to any printed copies of the source code brought to the deposition, the Producing Party would be required to bring a computer containing the source code (or otherwise transport the source code) to the deposition. This would increase the danger of source code material being lost or stolen in transit, and thus frustrate the purpose of the original proposal. Plaintiff has not identified any reason, let alone a compelling one, for why printed copies of source code and a source code computer are both necessary for Plaintiff to conduct depositions in this case.

Furthermore, Plaintiff's proposal fails to account for the location of witnesses in this action. Several of the Defendants are based overseas, and as a result, there may be witnesses deposed overseas. Plaintiff's proposal is would force the Producing Parties to provide source code computers at locations other than the source code inspection locations. The Producing Party should have the opportunity to determine whether provision of a source code computer, or printed copies of the previously-identified source code, would better protect its interests; this proposal does not in any way impede Plaintiff's ability to take depositions. In contrast, Plaintiff's proposal would require the Producing Party to place its source code at even greater risk multiple times throughout discovery, without any justification.

17. Paragraph 11(xi) - Disclosure and Review of Source Code

Plaintiff's Proposal	Defendants' Proposal
No provision.	Except as required for filings under seal with the Court, the Receiving Party may only create an electronic image of a selected portion of the Source Code when the electronic file containing such image has been encrypted using commercially reasonable encryption software including password protection.

Plaintiff's Statement:

ContentGuard respectfully opposes the additional language proposed by Defendants for two reasons. First, Defendants' proposal deviates from the Model Protective Order. Second, Defendants' proposal introduces needless, involved logistics related to the use of source code. The protections already built into the Protective Order are sufficient to safeguard Defendants' source code.

Defendants' Statement:

Defendants' overview concerning Plaintiff's proposals to substantially weaken the protections for source code is set forth in Section 10(c)(ii), above. Because Section 11(c)(iv) provides for Plaintiff's counsel to receive and maintain limited copies of source code, it is imperative that the protective order make clear that electronic images of any source code are only permitted under very limited and specified conditions. Defendants' proposal is reasonable in that it allows creation of such limited and controlled images, while also ensuring that any image is encrypted.

18. Paragraph 12(a) – Third-Party Confidentiality Obligations

Plaintiff's Proposal	Defendants' Proposal
Any party to this action intending to disclose third-party confidential information pursuant to this Order must first provide a copy of this Order and a list of specific items to be disclosed to such third-party. Such third-party is afforded fourteen (14) days to file a written objection with the Court should it wish to oppose the disclosure of such information. If no objection is received from such third-party within such fourteen (14) day time-period, the underlying information must immediately be produced. At the request of the Receiving Party, the producing party, prior to actual production, shall file a notice with the Court evidencing its compliance with this Order and verifying the date and method by which it gave notice to such affected third parties. Such notice may be filed under seal to protect any confidential information that might be included or disclosed in such notice. In any event, no disclosure is required until the objection is resolved.	For third-party confidential information not subject to another court-ordered protective order, any party to this action intending to disclose third-party confidential information pursuant to this Order must first provide a copy of this Order and a list of specific items to be disclosed to such third-party. Such third-party or the party to this action that received the request are afforded twenty-eight (28) days to file a written objection with the Court should one or both wish to oppose the disclosure of such information. If no objection is received within such twenty-eight (28) day time-period, and provided that production will not result in a violation of a contractual obligation with the third party, the underlying information must immediately be produced. The producing party, prior to actual production, shall file a notice with the Court evidencing its compliance with this Order and verifying the date and method by which it gave notice to such affected third parties. Such notice may be filed under seal to protect any confidential information that might be included or disclosed in such notice. In any event, no disclosure is required until the objection is resolved.

Plaintiff's Statement:

ContentGuard's proposal includes verbatim a portion of an order issued by this Court under Docket Number 264 in *Wi-LAN, Inc. v. HTC Corporation*, et al., Case 2:12-cv-00600-JRG. As it did in the *Wi-LAN* case, a provision setting a specific deadline by which third parties have to either consent to production or seek relief is certain to streamline discovery by incentivizing third parties to provide prompt feedback to production requests received from both ContentGuard and Defendants. ContentGuard's approach is tried-and-true and, since it applies

to all parties, fair. In contrast, Defendants' competing proposal is illusory because it allows the parties to indefinitely delay producing documents that contain third-party information if production would "result in a violation of a contractual obligation with a third party."

Defendants' Statement:

Plaintiff's proposal sets up a dangerous and unnecessary situation in which a party would have to choose whether to violate its existing contractual confidentially obligations with third parties or to violate this Protective Order. That is, Plaintiff's provision requires a party to produce third-party confidential information in its possession after expiration of an objection period, regardless of any contractual obligation that party has to maintain the confidentiality of the information. The Protective Order establishes a mechanism by which the confidentiality of information may be maintained, but it does not provide an escape hatch for a party's previously existing contractual obligations. Even if a third party declines to object to production during the notice period, that third party can still hold the producing party accountable for violating any contractual duties it had to keep the information secure. Defendants' proposal recognizes that issue and allows a party to preserve the sanctity of its contractual obligations.

This Court's Order in the *Wi-Lan, Inc. v. HTC Corp, et. al* and *Wi-Lan, Inc. v. Apple, Inc, et al.* cases (2:11-cv-600, D.I. 264), cited by ContentGuard, addressed a situation in which documents were subject to confidentially under a another protective order entered by the same Court. In that case, the parties to the protective order were already before this Court, albeit in different cause numbers. That situation is very different from Plaintiff's proposal, which attempts to trump third parties' existing rights of confidentiality without those entities being parties to this agreement or subject to the Order as entered by the Court. The appropriate route

for parties to obtain confidential documents from third parties is discovery pursuant to Rule 45 of the Federal Rules of Civil Procedure, not through forced contractual violations.

19. Paragraph 13(a)(iv) – Notice of Disclosure

Plaintiff's Proposal	Defendants' Proposal
Prior to disclosing any Protected Material to any person described in Paragraphs **Error! Reference source not found.**, 0, **Error! Reference source not found.**or **Error! Reference source not found.** (referenced below as "Person"), the Party seeking to disclose such information shall provide the Producing Party with written notice that includes: . . . (iv) an identification of all of the Person's past and current employment and consulting relationships, within the past <u>three (3) years</u>, including direct relationships and relationships through entities owned or controlled by the Person, including but not limited to an identification of any individual or entity with or for whom the person is employed or to whom the person provides consulting services relating to the design, development, operation, or patenting of digital rights management ("DRM") or relating to the acquisition of intellectual property assets relating to digital rights management ("DRM");	Prior to disclosing any Protected Material to any person described in Paragraphs **Error! Reference source not found.**, 0, **Error! Reference source not found.**or **Error! Reference source not found.** (referenced below as "Person"), the Party seeking to disclose such information shall provide the Producing Party with written notice that includes: . . . (iv) an identification of all of the Person's past and current employment and consulting relationships, within the past <u>five (5) years</u>, including direct relationships and relationships through entities owned or controlled by the Person, including but not limited to an identification of any individual or entity with or for whom the person is employed or to whom the person provides consulting services relating to the design, development, operation, or patenting of digital rights management ("DRM") <u>and digital content distribution systems and methods, including associated software and hardware,</u> or relating to the acquisition of intellectual property assets relating to digital rights management ("DRM") <u>and digital content distribution systems and methods, including associated software and hardware;</u>

<u>Plaintiff's Statement:</u>

ContentGuard proposes that disclosures be limited to current and past employment and consulting relationships going back three years. Defendants' proposal calling for information reaching back five years is overly broad and unnecessary. Furthermore, Defendants' proposal that the disclosure extend to engagements involving "associated software and hardware" is

overly broad. In this case, ContentGuard accuses specific DRM features, functionalities, and products. Extending disclosures to include "associated software and hardware," a term that could include any electronic device that has some DRM features, exponentially increases the number relationships to be disclosed beyond what is relevant to this litigation.

Defendants' Statement:

Defendants' position concerning Plaintiffs' effort to exclude from the protective order confidential and trade secret material relating to technologies Plaintiff has accused is set forth in Section 6(b), above.

In addition, providing a disclosure of consulting relationship for the past five years is fairly standard, not burdensome, and important to assess the risk of the expert advising Defendants' direct competitors on the same technology at issue here. *See, e.g.*, United States District Court for the Northern District of California, Patent Local Rule 2-2 Interim Model Protective Order (Oct. 10, 20113) at 11 (requiring experts with access to source code to disclose consulting engagements for past five years), available at:

http://www.cand.uscourts.gov/stipprotectorder.

20. Paragraph 13(a) – Notice of Disclosure

Plaintiff's Proposal	Defendants' Proposal
Further, the Party seeking to disclose Protected Material shall provide such other information regarding the Person's professional activities reasonably requested by the Producing Party for it to evaluate whether good cause exists to object to the disclosure of Protected Material to the outside expert or consultant. During the pendency of this action, including all appeals, the Party seeking to disclose Protected Material shall, immediately provide written notice of any change with respect to the Person's involvement in the design, development, operation or patenting of digital rights management ("DRM") or the acquisition of intellectual property assets relating to digital rights management ("DRM").	Further, the Party seeking to disclose Protected Material shall provide such other information regarding the Person's professional activities reasonably requested by the Producing Party for it to evaluate whether good cause exists to object to the disclosure of Protected Material to the outside expert or consultant. During the pendency of this action, including all appeals, the Party seeking to disclose Protected Material shall, immediately provide written notice of any change with respect to the Person's involvement in the design, development, operation or patenting of digital rights management ("DRM") and digital content distribution systems and methods, including associated software and hardware, or the acquisition of intellectual property assets relating to digital rights management ("DRM") and digital content distribution systems and methods.

Plaintiff's Statement:

Plaintiff's statement is set forth in Disputed Provision 19 above.

Defendants' Statement:

Defendants' position concerning Plaintiffs' effort to exclude from the protective order confidential and trade secret material relating to technologies Plaintiff has accused is set forth in Section 6(b), above.

Dated: May 19, 2014

Respectfully submitted,

/s/ Sam Baxter

Samuel F. Baxter
State Bar No. 01938000
sbaxter@mckoolsmith.com
MCKOOL SMITH P.C.
104 East Houston, Suite 300
Marshall, Texas 75670
Telephone: (903) 923-9000
Facsimile: (903) 923-9099

ATTORNEY FOR CONTENTGUARD HOLDINGS, INC.

/s/ Jennifer H. Doan (with permission)

Jennifer H. Doan
State Bar No. 08809050
jdoan@haltomdoan.com
Haltom & Doan
6500 Summerhill Road, Suite 100
Texarkana, TX 75503
(903) 255-1000
Fax: (903) 255-0800

ATTORNEY FOR AMAZON.COM, INC.

/s/ Melissa Richards Smith (with permission)

Melissa Richards Smith
State Bar No. 24001351
melissa@gillamsmithlaw.com
Gillam & Smith, LLP
303 South Washington Avenue
Marshall, TX 75670
(903) 934-8450
Fax: (903)-934-9257

ATTORNEY FOR APPLE INC.

/s/ John S. Torkelson (with permission)

John S. Torkelson
State Bar No. 00795154
jtorkelson@carterscholer.com
Carter Scholer Stafford Arnett Hamada & Mockler PLLC
8150 N. Central Expressway, Suite 1950
Dallas, TX 75206
(214) 550-8162
Fax: (214) 550-8185

ATTORNEY FOR BLACKBERRY CORPORATION (F/K/A RESEARCH IN MOTION CORPORATION); BLACKBERRY LIMITED (F/K/A RESEARCH IN MOTION LIMITED)

/s/ Eric H. Findlay (with permission)

Eric H. Findlay
State Bar No. 00789886
efindlay@findlaycraft.com
Findlay Craft, P.C.
102 North College Ave., Suite 900
Tyler, TX 75702
(903) 534-1100
Fax: (903) 534-1137

ATTORNEY FOR HTC CORPORATION AND HTC AMERICA, INC.

/s/ Scott F. Partridge (with permission)

Scott F. Partridge
State Bar No. 00786940
scott.partridge@bakerbotts.com
Baker Botts LLP
910 Louisiana, Suite 3000 One Shell Plaza
Houston, TX 77002-4995
(713) 229-1569
Fax: (713) 229-7769

ATTORNEY FOR HUAWEI DEVICE USA, INC. AND HUAWEI TECHNOLOGIES CO., LTD.

/s/ J. Mark Mann (with permission)

J. Mark Mann
State Bar No. 12926150
Mark@TheMannFirm.com
MANN, TINDEL. THOMPSON
300 West Main Street
Henderson, Texas 75652
(903) 657-8540
Fax: (903) 657-6003

ATTORNEY FOR MOTOROLA MOBILITY LLC

/s/ Michael E. Jones (with permission)

Michael E. Jones
State Bar No. 10929400
mikejones@potterminton.com
POTTER MINTON, PC
110 North College, Suite 500
Tyler, Texas 75702
(903) 597-8311
Fax: (903) 593-0846

ATTORNEY FOR SAMSUNG ELECTRONICS CO., LTD.; SAMSUNG ELECTRONICS AMERICA, INC.; SAMSUNG TELECOMMUNICATIONS AMERICA, LLC

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule CV-5(a). As such, this document was served on all counsel who have consented to electronic services on May 19, 2014. Local Rule CV-5(a)(3)(A).

/s/ Radu A. Lelutiu

CERTIFICATE OF CONFERENCE

Counsel for Plaintiff and counsel for Defendants have discussed the matters herein and have agreed to this joint filing.

/s/ Radu A. Lelutiu